

Ultra Low-Power implementation of ECC on the ARM Cortex-M0+

Ruan de Clercq, Leif Uhsadel, Anthony Van Herrewwege, Ingrid Verbauwhede
K.U. Leuven, Department of Electrical Engineering - ESAT/COSIC and iMinds
Kasteelpark Arenberg 10, 3001 Heverlee-Leuven, Belgium.
firstname.lastname@esat.kuleuven.be

ABSTRACT

In this work, elliptic curve cryptography (ECC) is used to make a fast, and very low-power software implementation of a public-key cryptography algorithm on the ARM Cortex-M0+. An optimization of the López-Dahab field multiplication method is proposed, which aims to reduce the number of memory accesses, as this is a slow operation on the target platform. A mixed C and assembly implementation was made; a random point multiplication requires 34.16 μ J, whereas our fixed point multiplication requires 20.63 μ J. Our implementation's energy consumption beats all other software implementations, on any platform, by a factor of at least 3.3.

Categories and Subject Descriptors: D.4.6 [Operating Systems]: Security and Protection—*Cryptographic Controls*

General Terms: Design, Security, Algorithms

Keywords: ECC, Public-key cryptography, Embedded, Low-Power

1. INTRODUCTION

A typical application for public-key cryptography in the ultra low-power domain is for Wireless Sensor Networks (WSNs). A WSN is an ad-hoc wireless network that consists of a number of nodes and one or more base stations. WSNs require security, because they communicate through an insecure channel while often operating unattended. As these devices are made to be economically viable, they have a limited amount of energy, computation power, memory and communication abilities. A node's lifetime is also directly influenced by the amount of energy that it uses to perform computations and is therefore also directly influenced by the efficiency of its algorithms.

ECC [15, 18] is an attractive option for Public-Key Cryptography on WSNs due to its lower computational and memory requirements, and is particularly useful in hybrid cryptosystems where PKC is used for key exchange, and symmetric cryptography is used for the efficient encryption of data.

Permission to make digital or hard copies of all or part of this work for personal or classroom use is granted without fee provided that copies are not made or distributed for profit or commercial advantage and that copies bear this notice and the full citation on the first page. Copyrights for components of this work owned by others than ACM must be honored. Abstracting with credit is permitted. To copy otherwise, or republish, to post on servers or to redistribute to lists, requires prior specific permission and/or a fee. Request permissions from Permissions@acm.org.

DAC '14 June 01 - 05 2014, San Francisco, CA, USA

Copyright 2014 ACM 978-1-4503-2730-5/14/06\$15.00.

<http://dx.doi.org/10.1145/2593069.2593238>.

The ARM Cortex-M0+ [2] is a low cost, ultra low-power microcontroller (MCU) with a 32-bit architecture, and a small but powerful instruction set. The authors are convinced that this platform is appropriate for WSNs not only because of its specs, but also because first integrations of this MCU have already been announced [9]. As this processor has only been available since 2012, we do not know of any other PKC implementations optimized for this architecture.

We now present the new state of the art in low-power software implementations of ECC on the ARM Cortex-M0+. In particular, we propose an optimization of the López-Dahab (LD) [16] field multiplication, which aims to reduce the number of memory accesses, as this is a slow operation on the target platform. The results will be compared to the existing solutions in the ultra low-power domain, as well as to a standard library compiled for this MCU.

The rest of the paper is organized as follows. First, we will discuss related work in the low-power domain in section 2. Following we discuss the methods that were used to perform the parameter, and algorithmic selection for our implementation in section 3. Next, we describe our results, and compare them with the results from implementations found in literature and in software libraries in section 4. Subsequent, we discuss some ideas for future work in section 5, and finally we provide a general conclusion in section 6.

2. RELATED WORK

Here we will discuss the related work of low-power software implementations of ECC. There is an evolution of algorithms and hardware, and therefore the overview follows a chronological order, with a focus on the López-Dahab (LD) [16] field multiplication method, as our implementation is based on this. The LD method and window parameter w will be discussed in more detail later. A number of low-power implementations exist in the literature; however, in the past a lot of the focus has gone towards software implementations on existing WSNs like the 8-bit MICA2 and MICAz (which both contain the ATmega128L) and the 16-bit TelosB (which contains the MSP430). Only a small number of implementations were found in the literature for ARM MCUs like the IMote2 (which contains the ARMv5TE based PXA271), and the ARM7TDMI.

Gura et al. [11] showed that by optimizing the number of memory accesses, which are often the most expensive operation on an MCU, significant gains in performance can be achieved.

Szczechowiak et al. [23] made binary curve, and prime curve implementations for the Tmote Sky and the MICA2,

based on the MIRACL library. Multiplication on prime curves use Hybrid multiplication [11], and multiplication on binary curves use the Karatsuba-Ofman multiplication algorithm. For binary fields they used binary Koblitz curves as no expensive doubling operations are required. For fixed point multiplication in prime fields they perform pre-computation with the Comb method and $w = 4$. Their point multiplications in prime fields was found to be faster than in binary.

Kargl et al. made software implementations on the ATMega128L for prime, and binary fields [14]. For multiplication in the binary field they use LD with $w = 4$, and a Montgomery-ladder algorithm which provides a constant execution time for point multiplication.

B. Oliveira et al. [20] made an implementation for the PXA27x on an underlying binary field of order 2^{271} . They made an optimization of the LD algorithm, called the **LD with rotating registers** method. They also performed immediate reduction of the upper half of the words instead of writing them to memory for later reduction. Assembly optimizations were used for field arithmetic.

P. Szczechowiak et al. [22] made an implementation in 2^{271} that uses the LD with $w = 8$, and 2-bit scanning. Two pointers are used to access the appropriate bytes in memory, thereby avoiding a multi-precision shift of the partial product vector.

Aranha et al. [7] made an optimization to the LD algorithm, called **LD with rotating registers**, where the memory accesses to intermediate values are reduced by making use of a rotating register scheme. In their implementation on the ATMega128L, they interleave multiplication with the reduction operation, and modular squaring is done with the table-based method interleaved with the reduction step so that the upper half of the words which are produced by squaring doesn't need to be written to memory.

S. Erdem [8] made several binary curve implementations for the ARM7TDMI using the operand-scanning method combined with LD with $w = 4$.

Gouvea et al. [10] made implementations on prime curves, binary curves, and binary Koblitz curves for MSP430 MCUs. Comba [6] multiplication is used for 160-bit prime curves, and Karatsuba-Ofman [13] multiplication is used for 256-bit prime curves. For binary fields they use LD multiplication for the 163-bit underlying field, and Karatsuba-Ofman with LD for the 283-bit underlying field.

Wenger et al. [24] made a number of ECC implementations for the ATMega128, MSP430, and Cortex M0+. They used cycle-accurate VHDL clones to evaluate the runtime, chip area, power, and energy characteristics of ECC implementations.

3. METHODS

In this section, we present the methods that were used to perform the parameter and algorithmic selection that is necessary to make an efficient and low-power ECC implementation. First, we will discuss the model that was used to make a curve selection. Next, we will discuss some of the algorithmic choices that were made.

3.1 Matching a curve to the architecture

In order to make an efficient and low-power implementation it is necessary to select the appropriate curve for the

architecture of the target platform. A model was made to determine the instruction usage, cycle count, and energy usage of a specific curve. For the model we considered only Binary Koblitz, and prime curves. Efficient algorithms and coordinate systems were selected to perform a point multiplication. The core of this model consisted of an analysis of the instructions required for performing a field multiplication algorithm, as this is most dominant routine in terms of execution time in an ECC. From this the execution times for performing a point multiplication were estimated, and we came to two conclusions that are relevant for the target platform: (1) Binary Koblitz curves will lead to a slightly faster implementation (2) Binary curves require less power than prime curves, because binary curve arithmetic consist largely of XOR and shift instructions, whereas prime curve arithmetic consist mostly of multiply and add instructions. The energy profiling results of the target platform (section 4.1) show that both the shift, and XOR instructions require less energy than either the multiply, and ADD instructions.

3.2 Field arithmetic algorithms

Here we will discuss some of the different field arithmetic algorithms that were used during analysis and implementation.

3.2.1 Multiplication

Field multiplication computes $x(z) \cdot y(z)$, where $x(z)$ and $y(z)$ are two binary polynomials of degree at most $m - 1$.

The López-Dahab (LD) field multiplication algorithm is a windowed multiplication algorithm for \mathbb{F}_{2^m} . The number of multi-precision shift operations is reduced by scanning the input parameter x with w bits at a time. Each w bits are then used to perform a table lookup, and the number of outer loop iterations are reduced to only $\lceil W/w \rceil$, where W is the word size of the processor. The lookup table is computed with $T(u) \leftarrow u(z) \cdot y(z)$ for all polynomials $u(z)$ of degree lower than w . The number of words required to store the lookup table is given by:

$$\begin{cases} 2^w(n+1) & , \text{ if degree}(y) > nW - (w-1), \\ 2^w(n) & , \text{ if degree}(y) \leq nW - (w-1), \end{cases} \quad (1)$$

where n is the number of words needed for the field parameter. While generating the lookup table, y is left-shifted by a maximum amount of $w - 1$ bits, which may cause a large polynomial to overflow into another word.

We propose a new optimization to the (LD) field multiplication algorithm, and call it the **López-Dahab with fixed registers** method. This algorithm aims to reduce the number of memory operations by keeping as many words of the internal state vector as possible inside registers. The most frequently used words are stored inside fixed register positions, and the least frequently used words are stored inside memory. On the target platform it is feasible to store a maximum of nine words inside registers.

Algorithm 1 shows the **LD with fixed registers** for $n = 8$, and a register count of $n + 1$. The parameter v denotes the internal state vector of $2n$ words which contains the intermediate results, which are stored inside memory, as well as fixed register positions. The $n + 1$ most frequently used words are stored inside registers, denoted by r , and the remaining $n - 1$ words are stored inside memory, denoted by m .

It was observed that $v[3 \dots 12]$ are the most frequently used $n + 1$ elements and are therefore stored inside the registers. $v[0 \dots 2]$ and $v[12 \dots 15]$ are the least frequently used $n - 1$ elements inside v and are therefore stored inside memory.

Fig. 1 provides a visual representation of the algorithm. All the light colored squares represents words which are stored in memory, and all the dark colored squares represents words which are stored in registers. First the lookup table, indicated with LUT, is computed from the input parameter x . Each cell inside the LUT represents 8 words stored in memory. The vector C contains the partial products of the multiplication, and consists of words stored inside memory, as well as in registers. The vector y is split into sections of w bits, and these sections are used as an index into the LUT. The index is used to read a cell in the LUT, and add it to C . As each cell contains 8 words, 8 words are read from the LUT, and then added to C . The lookup and add process is repeated 8 times, each time offset by one more word. After the eighth lookup, C is left shifted by 4 bits. This is repeated 8 times, but in the final iteration the shift is not required.

In order to reduce the number of memory operations the field multiplication algorithm can be interleaved with the reduction algorithm.

Algorithm 1 López-Dahab with fixed registers multiplication in \mathbb{F}_{2^m} for $n = 8$.

Input: $x(z) = x[0 \dots n - 1], y(z) = y[0 \dots n - 1]$
Output: $v(z) = v[0 \dots 2n - 1] = x(z)y(z)$
Note: v denotes the internal state vector composed of $n - 1$ memory addresses and $n + 1$ registers. $v \leftarrow (m[0], m[1], m[2], r_0, r_1, \dots, r_n, m[3], m[4], m[5], m[6])$.

```

1: Compute  $T(u) \leftarrow u(z)y(z)$  for all polynomials  $u(z)$  of
   degree lower than  $w$ 
2:  $v[0 \dots 2n - 1] \leftarrow 0$ 
3: for  $j \leftarrow \lceil W/w \rceil - 1$  downto 0 do
4:   for  $k \leftarrow 0$  to  $n - 1$  do
5:      $u = (x[k] \gg j \cdot W) \& 0xF$ 
6:     for  $l \leftarrow 0$  to  $n - 1$  do
7:        $v[l + k] \leftarrow v[l + k] \oplus T[u][l]$ 
8:     end for
9:   end for
10:  if  $(j \neq 0)$  then
11:     $v(z) = v(z) \cdot z^w$ 
12:  end if
13: end for
14: return  $v$ 

```

3.2.2 Reduction

Since the curve we are using has a sparse reduction polynomial, the reduction can be efficiently computed one word at a time.

3.2.3 Inversion

Inversion is done by means of the Extended Euclidean Algorithm [12] for polynomials. This algorithm makes use of two multi-precision internal state variables (u and v). One expensive operation that is called for in the algorithm is swapping u with v . The swap operation can be avoided by writing two separate segments of code in which both segments perform the same operations, but where the names of

the variables are interchanged. This eliminates a large number of expensive memory operations. Another optimization is to use two variables to store the index of the most significant non-zero word of u and v . This allows for performing a fast calculation of the degree of the polynomial and a reduced number of memory operations in the variable field shift function.

3.2.4 Squaring

Squaring is done by means of a 16-bit lookup table with 256 entries, requiring 4 kB. To reduce redundant memory operations, modular reduction is interleaved with the squaring functions. The lower half of the output of the squaring operation is kept inside the registers and the upper half is expanded and then immediately reduced. The upper half of the elements are therefore not required to be stored first and reduced later.

3.3 Comparison of multiplication algorithms

The field multiplication routine is the most dominant in terms of execution time in an ECC system. We will now compare our proposed optimization of the LD algorithm to the previous best method (the LD with rotating registers), as well as the original LD algorithm.

For all three methods a window size of $w = 4$ is used, where a single precomputation table of $16n$ words (4 kB) is required. This is valid under the assumption that the scalar y is short. For both the analysis of the LD with rotating registers, and the LD with fixed registers methods, we assume that $n + 1$ registers are available for storing the partial products.

Table 1. Estimated required operation formulas for field multiplication in $\mathbb{F}_{2^{233}}$.

Method	Read	Write	XOR
A	$16n^2 + 23n$	$8n^2 + 30n$	$8n^2 + 30n - 7$
B	$8n^2 + 39n - 8$	$46n$	$8n^2 + 38n - 7$
C	$8n^2 + 24n + 1$	$31n + 1$	$8n^2 + 30n - 7$

Method A: LD

Method B: LD with rotating registers

Method C: LD with fixed registers

The number of shift operations remain constant at $42n - 21$ for all three methods.

Table 2. Estimated required operations for field multiplication in $\mathbb{F}_{2^{233}}$.

Method	Read	Write	XOR	Shift	Total[cycles]*
A	1208	752	745	315	4980
B	816	368	809	315	3492
C	705	249	745	315	2968

Method A: LD

Method B: LD with rotating registers

Method C: LD with fixed registers

The total number of shift operations is constant at $42n - 21$ for all three methods

* Memory operations are assumed to require two cycles per operation.

The total number of operations and cycle estimates are shown in Table 1 and Table 2 respectively. The cycle estimate assumes that a memory operation will take 2 cycles and all other operations take only 1 cycle to complete.

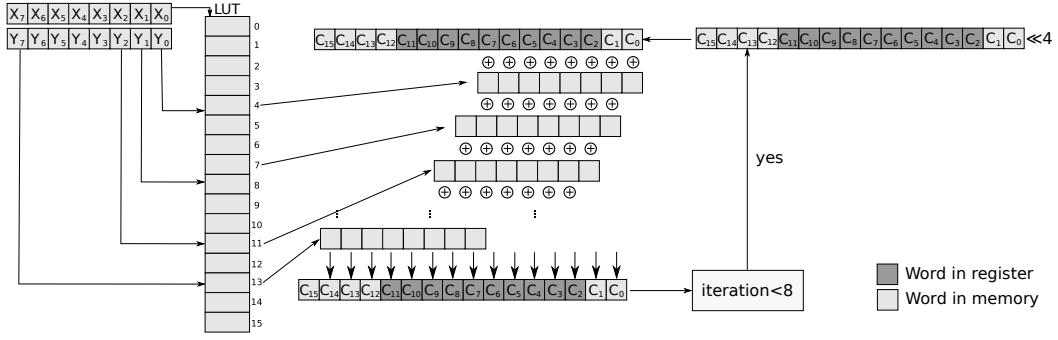


Figure 1. The proposed LD with fixed registers algorithm in \mathbb{F}_{2^m} for $n = 8$. The lookup table LUT is generated from the input scalar x . The main loop is executed 8 times for $w = 4$. The input parameter y is split up into sections of w bits which are used as an index for the LUT.

When comparing the LD method to the LD with rotating registers method, we see a drastic reduction in the number of memory operations due to the implementation of the rotating register scheme, which minimizes the storing of intermediate values in memory. When comparing the LD with fixed registers method to the LD with rotating registers, we see a further reduction of memory accesses due to the more efficient usage of registers. The LD with fixed registers has a performance increase of 15% over the LD with rotating registers method, and a performance increase of 40% over the standard LD method.

4. RESULTS

This section will be used to present our key results. First, we will discuss the measurements setup, and the results from our measurements. Next, we will present two implementations, and compare them to the state of the art low-power implementations found in literature, as well as with software libraries

4.1 Measurement setup and results

In order to determine the energy usage of different instructions as well as cryptographic software implementations, a system was designed to measure the power consumption of the target platform.

The power consumption for a number of different instructions were measured in order to investigate the effect of different field arithmetic algorithms on the overall power consumption. Table 3 shows the results of energy measurements for instructions which are relevant to prime and binary field arithmetic. A variation in energy consumption of up to 22.5% was observed between different instructions. The ADD instruction was found to be the most energy hungry, requiring 6.9% more energy than any other measured instruction. This is important for the choice of the underlying field because binary field arithmetic require a large amount of shift (LSL and LSR) and XOR instructions, whereas prime field arithmetic require a large amount of MUL and ADD instructions.

4.2 Comparison with other libraries

Table 4 and Table 5 shows our proposed implementation compared with low power implementations found in literature, as well as with software libraries. In the cases where the energy consumption was not provided in the author's

Table 3. The energy used per cycle for different instructions. The clock frequency is 48MHz.

Instruction	Energy [pJ]
LDR	10.98
LSR	12.05
MUL	12.14
LSL	12.21
XOR	12.43
ADD	13.45

results, the values are estimated from the typical energy consumption values found in [5, 21].

Most of the compared implementations use processors with different architectures, and different technology sizes. It would be possible to normalize the energy values, however as the technology sizes, and operating voltages of some of the implementations are not known, it is doubtful whether this would be a worthwhile exercise. Further, as an end user you often do not have the option of choosing the technology size of a given MCU. Therefore, comparing the energy usage of different implementations that use off-the-shelf MCUs is still valuable, as this gives an indication of the typical energy consumption of performing point multiplications on these MCUs.

Both the ARM7TDMI, and the PXA271 are more powerful platforms than the ARMv6-M based ARM Cortex-M0+ because they both have larger instruction sets which are capable of accessing all the registers, embedding shift instructions inside data processing instructions, and conditional execution of all instructions. However, the ARM Cortex-M0+ uses less energy per cycle than either the ARM7TDMI or the PXA271.

The MIRACL Crypto SDK [4] is an open-source Elliptic Curve Crypto SDK that supports many different platforms. It is a C library with some field arithmetic in assembly for many of its supported platforms. Some timings for this library can be found in [3] and are also listed in Table 4.

The RELIC toolkit [1] is an open-source cryptographic library that supports many different architectures.

Micro ECC [17] is a small, C-based, open-source library of ECDH and ECDSA for 32-bit microcontrollers.

In the following text we will present two implementations. First, we will present an implementation that relies exclusively on the RELIC toolkit to make all its computations. Next, we present an implementation that was largely developed in C and assembly, but also makes use of the RELIC toolkit to perform some calculations. The curve and algorithmic parameters for both implementations were chosen to

Table 4. Timings for point multiplications. All timings are given in milliseconds and energy is given in microjoules (μJ). The AT-Mega128L runs at 7.37MHz except when indicated with ^a, the MSP430 runs at 8.192MHz, the ARM7TDMI runs at 80MHz, and the ARM Cortex-M0+ runs at 48MHz.

Platform	Author	Curve	Multiply	
			[ms]	[μJ]
ARM7TDMI	MIRACL [3]	secp192r1	38 ^r	182.4 ^e
ARM7TDMI	MIRACL [3]	secp224r1	53 ^r	254.4 ^e
ATMega128L	Aranha et al. [7]	sect163k1	320 ^r	9600 ^e
ATMega128L ^a	Kargl et al. [14]	167-bit ^b	763 ^r	24840 ^e
ATMega128L	Aranha et al. [7]	sect233k1	730 ^r	21900 ^e
MSP430F1611	NanoECC [23]	P-160	720 ^f	8847 ^m
MSP430F1611	NanoECC [23]	sect163k1	1040 ^f	12780 ^m
Cortex-M0	Micro ECC [17]	secp192r1	175.7 ^f	134.9 ^e
Cortex-M0	Micro ECC [17]	secp256r1	465.1 ^f	357.2 ^e
Cortex-M0+	Wenger et al. [24]	secp224r1	693 ^r	496 ^m
Cortex-M0+	Relic kG	sect233k1	115.7 ^f	69.48 ^m
Cortex-M0+	Relic kP	sect233k1	117.1 ^r	70.26 ^m
Cortex-M0+	<i>This work</i> kG	sect233k1	39.70 ^f	20.63 ^m
Cortex-M0+	<i>This work</i> kP	sect233k1	59.18 ^r	34.16 ^m

^a Runs at 8MHz.

^m Energy measurement.

^e Energy estimation.

^m Energy measurement of cycle-accurate clone with 10MHz clock.

^f Fixed-point multiplication.

^p A custom prime curve is used.

^r Random point multiplication.

Table 5. Average cycle times for modular multiplication and modular squaring on different platforms.

Author	Platform	Word size	Sqr	Mul	Field
S. Erdem [8]	ARM7TDMI	32	348	4359	$\mathbb{F}_{2^{228}}$
S. Erdem [8]	ARM7TDMI	32	389	5398	$\mathbb{F}_{2^{256}}$
Aranha et al. [7]	ATMega128L	8	570	4508	$\mathbb{F}_{2^{163}}$
Aranha et al. [7]	ATMega128L	8	956	8314	$\mathbb{F}_{2^{233}}$
Kargl et al. [14]	ATMega128L	8	-	2593	\mathbb{F}_{160}
Kargl et al. [14]	ATMega128L	8	663	5490	$\mathbb{F}_{2^{167}}$
P. Szczechowiak et al. [22]	ATMega128L	8	1581	13557	$\mathbb{F}_{2^{271}}$
Gouvea [10]	MSP430X ^a	16	630	741	\mathbb{F}_{160}
Gouvea [10]	MSP430X ^a	16	199	3585	$\mathbb{F}_{2^{163}}$
Gouvea [10]	MSP430X ^a	16	1369	1620	$\mathbb{F}_{2^{256}}$
Gouvea [10]	MSP430X ^a	16	325	8166	$\mathbb{F}_{2^{283}}$
TinyPBC [20]	PXA271	32	187	2025	$\mathbb{F}_{2^{271}}$
TinyPBC [20]	PXA271 ^b	32	187	1411	$\mathbb{F}_{2^{271}}$
<i>This work</i>	Cortex-M0+	32	395	3672	$\mathbb{F}_{2^{233}}$

^a This model has a long 32-bit multiplier

^b This model (wMMX) has a SIMD instruction set.

match each other as close as possible.

4.2.1 RELIC implementation

The RELIC toolkit was used to make an implementation with the following configuration: a binary Koblitz curve of order 2^{233} is used. The left-to-right w TNAF method with $w = 4$ was used for point multiplication. Point additions are done in mixed LD-affine coordinates. Fast reduction is done because the reduction polynomial is trinomial. Inversion is performed with the Extended Euclidean algorithm and squaring is done using the table-based method.

The RELIC implementation was measured to have an average power consumption of 600 μW while performing a random point multiplication, and 600.5 μW while performing a fixed point multiplication. This implementation requires an average of 5621045 cycles, and 72.5 μJ for a random point multiplication, and only 5553828 cycles, and 71.6 μJ for a fixed point multiplication. The average cycle time and energy usage of this implementation is compared to others in

Table 4. Even though the fixed point multiplication uses more power than the random point multiplication, it still uses less energy because its faster.

4.2.2 Proposed implementation

An implementation was made using C and assembly that uses the binary Koblitz sect233k1 curve. The left-to-right w TNAF method was used for point multiplication; the parameter w was set to 4 for random point multiplication (kP), and $w = 6$ for fixed point multiplication (kG). Point additions are done in mixed LD-affine coordinates. The RELIC toolkit was used to perform the TNAF precomputation, and TNAF transformation of the scalar k . The LD with fixed registers method was used for field multiplication, reduction was done one word at a time, inversion was done with the Extended Euclidean algorithm, and squaring was done with the table-based method. The field arithmetic routines were written in C and assembly.

The average execution time and energy usage of this implementation is compared to others in Table 4 and Table 5. Our proposed implementation was measured to have an average power consumption of 577.2 μW for a random point multiplication, and 519.6 μW for a fixed-point multiplication. On average our random point multiplication implementation require 2814827 cycles, and 36.6 μJ , whereas our fixed point multiplication require 1864470 cycles, and 24.6 μJ . When compared to RELIC, our random point implementation is 1.99 times faster, and our fixed point implementation is 2.98 times faster. The field arithmetic cycle times are shown in Table 6, and the accumulated execution time for different operations are shown in Table 7 for both a random point multiplication (kP), as well as a fixed point multiplication (kG).

Table 6. Average cycle times for field arithmetic algorithms in $\mathbb{F}_{2^{233}}$.

Operation	C language	Assembly
Modular Squaring	419	395
Inversion	141 916	-
LD with rotating registers	5 592	-
LD with fixed registers	5 964	3 672
kP	3 516 295	2 761 640
kG	2 494 757	1 864 470

Table 7. Total accumulated timings per operation for random point multiplication (kP), and fixed point multiplication (kG).

Operation	kP	kG
TNAF Representation	178 135	185 926
TNAF Precomputation	398 387	0
Multiply	1 108 890	821 178
Multiply Precomputation	249 750	184 950
Square	362 379	342 294
Inversion	139 936	139 656
Support functions	377 350	376 392
Total	2 814 827	1 864 470

5. FUTURE WORK

The current implementation doesn't execute in constant-time and is therefore at risk of a power analysis attack. It would be very interesting to see the results of an implementation where the point multiplication routine is implemented in constant-time by using an algorithm like the Montgomery-Ladder [19] method.

6. CONCLUSION

We made an ECC implementation based on a binary Koblitz curve in $\mathbb{F}_{2^{233}}$, because we estimated that it will lead to a faster implementation with a lower energy consumption than a prime curve implementation with an equivalent security level. An optimization of the López-Dahab (LD) field multiplication method is proposed, called the López-Dahab with fixed registers. It is based on optimizing for memory accesses, which is the most expensive operation on the target platform. Our proposed algorithm has a cycle count of 3672 cycles, and a performance improvement of 15% over the LD with rotating registers [20] algorithm. Our implementation of a random point multiplication requires 2814827 cycles, and 34.16 μ J, whereas our fixed point multiplication requires 1864470 cycles, and 20.63 μ J. The energy consumption of our point multiplication implementation beats all known software implementations on any embedded platform, on the same equivalent security level, by a factor of at least 3.3.

Acknowledgment

This work was supported in part by the Research Council KU Leuven: GOA TENSE (GOA/11/007). In addition, this work is supported in part by the Flemish Government, FWO G.0550.12N, G.00130.13N and FWO G.0876.14N, by the Hercules Foundation AKUL/11/19, and in part by the Erasmus Mundus Action 2 South Africa (ema2sa) project.

References

- [1] D. Aranha and C. P. L. Gouvêa. RELIC Cryptographic Toolkit. <https://code.google.com/p/relic-toolkit/>, 2013. Accessed: 2013-05-28.
- [2] ARM. Cortex-M0+ Technical Reference Manual, Revision: r0p1. http://infocenter.arm.com/help/topic/com.arm.doc.ddi0484c/DDI0484C_cortex_m0p_r0p1_trm.pdf, 2012. Accessed: 2013-06-06.
- [3] Certivox Ltd. Benchmarks and Subs. <https://wiki.certivox.com/display/EXT/Benchmarks+and+Subs>, 2012. Accessed: 2013-05-28.
- [4] Certivox Ltd. MIRACL Cryptographic Library. <https://certivox.com/solutions/miracl-crypto-sdk/>, 2013. Accessed: 2013-05-28.
- [5] D. Chinnery and K. Keutzer. Closing the power gap between ASIC and custom: an ASIC perspective. In *Proceedings of the 42nd annual Design Automation Conference*, pages 275–280. ACM, 2005.
- [6] P. G. Comba. Exponentiation cryptosystems on the IBM PC. *IBM systems journal*, 29(4):526–538, 1990.
- [7] D. Aranha, L. Oliveira, J. López, and R. Dahab. Efficient implementation of elliptic curve cryptography in wireless sensors. *Advances in Mathematics of Communications*, 4(2):169–187, 2010.
- [8] S. Erdem. Fast software multiplication in $\mathbb{F}_2[x]$ for embedded processors. *Turkish Journal of Electrical Engineering & Computer Sciences*, 2012.
- [9] Freescale Semiconductor Inc. MKW01Z128, Highly-integrated, cost-effective single-package solution for sub-1 GHz applications, Rev. 3, 5/7/2013. 2013.
- [10] C. Gouvêa, L. Oliveira, and J. López. Efficient software implementation of public-key cryptography on sensor networks using the MSP430X microcontroller. *Journal of Cryptographic Engineering*, 2(1):19–29, 2012.
- [11] N. Gura, A. Patel, A. Wander, H. Eberle, and S. Shantz. Comparing elliptic curve cryptography and RSA on 8-bit CPUs. In *Cryptographic Hardware and Embedded Systems-CHES 2004*, pages 119–132. Springer, 2004.
- [12] D. Hankerson, A. Menezes, and S. Vanstone. *Guide to Elliptic Curve Cryptography*. Springer-Verlag New York, Inc., Secaucus, NJ, USA, 2003.
- [13] A. Karatsuba and Y. Ofman. Multiplication of multi-digit numbers on automata. In *Soviet physics doklady*, volume 7, page 595, 1963.
- [14] A. Kargl, S. Pyka, and H. Seuschek. Fast arithmetic on ATmega128 for elliptic curve cryptography. *International Association for Cryptologic Research Eprint archive*, 2008.
- [15] N. Koblitz. Elliptic Curve Cryptosystems. *Mathematics of Computation*, 48(177):203–209, Jan. 1987.
- [16] J. López and R. Dahab. High-speed software multiplication in \mathbb{F}_{2^m} . In *Progress in Cryptology-INDOCRYPT 2000*, pages 203–212. Springer, 2000.
- [17] K. MacKay. micro ecc. <https://github.com/kmackay/micro-ecc>, 2014. Accessed: 2014-03-25.
- [18] V. Miller. Use of elliptic curves in cryptography. In *Lecture notes in computer sciences; 218 on Advances in cryptology—CRYPTO 85*, pages 417–426, New York, NY, USA, 1986. Springer-Verlag New York, Inc.
- [19] P. Montgomery. Speeding the Pollard and Elliptic Curve Methods of Factorization. *Mathematics of computation*, 48:243–264, 1987.
- [20] L. Oliveira, M. Scott, J. López, and R. Dahab. TinyPBC: Pairings for authenticated identity-based non-interactive key distribution in sensor networks. In *In Networked Sensing Systems, 2008. INSS 2008. 5th International Conference on*, pages 173–180, 2008.
- [21] K. Piotrowski, P. Langendoerfer, and S. Peter. How public key cryptography influences wireless sensor node lifetime. In *Proceedings of the fourth ACM workshop on Security of ad hoc and sensor networks*, SASN ’06, pages 169–176, New York, NY, USA, 2006. ACM.
- [22] P. Szczechowiak, A. Kargl, M. Scott, and M. Collier. On the application of pairing based cryptography to wireless sensor networks. In *Proceedings of the second ACM conference on Wireless network security*, pages 1–12. ACM, 2009.
- [23] P. Szczechowiak, L. Oliveira, M. Scott, M. Collier, and R. Dahab. NanoECC: Testing the Limits of Elliptic Curve Cryptography in Sensor Networks. In *EWSN*, volume 4913 of *Lecture Notes in Computer Science*, pages 305–320. Springer, 2008.
- [24] E. Wenger, T. Unterluggauer, and M. Werner. 8/16/32 shades of elliptic curve cryptography on embedded processors. In *Progress in Cryptology-INDOCRYPT 2013*, pages 244–261. Springer, 2013.